

Ontologia para representação do conhecimento sobre consentimento do titular de dados pessoais em mídias sociais digitais

Camila Gourgues Pereira^{1*}, Luciano Heitor Gallegos Marin¹ and Cristina Godoy Bernardo de Oliveira²

¹ Federal University of Paraná (UFPR), Prefeito Lothário Meissner Av., 632, 80210-170, Curitiba, PR, Brazil

² University of São Paulo (USP), Bandeirantes Av., 3900, 14040-906, Ribeirão Preto, SP, Brazil

Resumo

As mídias sociais digitais transformaram as formas de interação e comunicação na sociedade contemporânea, ao mesmo tempo em que intensificaram a coleta e o uso de dados pessoais. Nesse contexto, uma das bases legais para o tratamento de dados pessoais é o consentimento do usuário, conforme previsto na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). No entanto, fatores como a assimetria de poder, a complexidade das políticas de privacidade, a presença de *dark patterns* e os vieses cognitivos dificultam que o consentimento seja realmente livre, informado e inequívoco, conforme previsto em Lei. Esta pesquisa em desenvolvimento, de caráter descritivo, utiliza a metodologia *OntoForInfoScience* para o desenvolvimento de uma estrutura semântica ontológica voltada à representação do consentimento do titular de dados pessoais em mídias sociais digitais. A proposta integra fundamentos legais e aspectos sociocomportamentais, com o objetivo de oferecer uma estrutura semântica visando apoiar soluções tecnológicas para a privacidade de dados pessoais, a conformidade normativa e a conscientização dos usuários.

Palavras-chave

Ontologia, Consentimento, Mídias Sociais Digitais, Proteção de Dados

Abstract

Digital social media has reshaped interaction and communication in contemporary society, while simultaneously intensifying the collection and use of personal data. In this context, consent represents one of the legal bases for processing personal data, as established by the Brazilian General Data Protection Law (Law No. 13,709/2018). However, factors such as power asymmetry, the complexity of privacy policies, the presence of dark patterns, and cognitive biases often prevent consent from being truly free, informed, and unambiguous, as required by law. This descriptive, ongoing research employs the *OntoForInfoScience* methodology to develop an ontological semantic structure aimed at representing data subjects' consent in digital social media. The proposal integrates legal foundations and socio-behavioral aspects, aiming to provide a semantic framework to support technological solutions for personal data privacy, regulatory compliance, and user awareness.

Keywords

Ontology, Consent, Digital Social Media, Data Protection

1. Introdução

A crescente digitalização da vida social é impulsionada pela convergência das tecnologias da informação e da globalização econômica, que promovem transformações na forma como os indivíduos se relacionam e interagem. Consolida-se, assim, uma nova rede global de comunicação e informação, formada por plataformas de mídias sociais e por dispositivos móveis, em que todos os aspectos da vida social estão interconectados [1].

Proceedings of the 18th Seminar on Ontology Research in Brazil (ONTOBRAS 2025) and 9th Doctoral and Masters Consortium on Ontologies (WTD0 2025), São José dos Campos (SP), Brazil, September 29 – October 02, 2025.

* Corresponding author.

✉ camilagourgues@ufpr.br (C. G. Pereira); luciano.gallegos@ufpr.br (L. H. G. Marin); cristinagodoy@usp.br (C. G. B. Oliveira)

ORCID 0009-0000-8352-2362 (C. G. Pereira); 0000-0002-4331-6588 (L. H. G. Marin); 0000-0003-4590-3249 (C. G. B. Oliveira)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

Nesse contexto, as mídias sociais digitais redefiniram as formas de interação social e tornaram-se centrais na sociedade moderna como espaços de conexão, interação e negócios [2]. Os usuários, ao interagirem com essas tecnologias, recebem e enviam uma grande quantidade de dados, os quais fornecem detalhes de sua vida privada e de suas preferências pessoais. Por conseguinte, essas plataformas formam uma grande rede informacional, na qual circula uma quantidade excessiva de dados e informações a todo momento [1].

Essa dinâmica de fluxo informacional é central na chamada “economia digital”, na qual tecnologias de Inteligência Artificial, Internet das Coisas e Big Data dependem do acesso e da análise de dados pessoais para oferecer serviços personalizados. No entanto, tal prática expõe os indivíduos a um monitoramento contínuo que pode infringir a liberdade e gerar risco de vazamento de informações [3]. Como resultado, a coleta e o uso indiscriminado de dados pessoais pelas mídias sociais digitais podem representar riscos à proteção de dados e à privacidade dos usuários [2].

Diante do panorama apresentado, nos últimos anos, a proteção de dados pessoais se consolidou como uma questão global de relevância pública e jurídica. Assim, diversos países promulgaram suas próprias legislações sobre o tema [3]. Como marco importante, pode-se citar o General Data Protection Regulation (GDPR), que entrou em vigor em 2018, o regulamento da União Europeia que afeta qualquer empresa ou organização que trate dados de cidadãos europeus, independentemente de onde esteja localizada [4].

Foi nesse cenário que, no Brasil, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), foi sancionada em 2018. A LGPD, inspirada pelo GDPR, estabelece princípios, direitos e deveres aplicáveis ao tratamento de dados pessoais, buscando garantir o respeito à autodeterminação informativa dos titulares. No contexto atual, o **consentimento do titular** destaca-se como uma das bases legais para o tratamento de dados, sendo compreendido como a concordância do titular de dados com o tratamento de seus dados, por meio de uma manifestação livre, informada e inequívoca, com uma finalidade específica [5].

No entanto, embora o consentimento seja exigido, inclusive em mídias sociais digitais, para o tratamento de dados dos usuários, frequentemente há uma assimetria de informações e de poder nas plataformas. Os usuários, embora teoricamente informados sobre as formas de tratamento de dados por meio das políticas de privacidade, muitas vezes não estão plenamente cientes de como ocorrem, de fato, a coleta, o uso e o compartilhamento de seus dados [2]. Isso ocorre principalmente devido ao volume e à complexidade dos termos e condições de uso e políticas de privacidade, que, além de conterem termos técnicos e complexos que muitos indivíduos não compreendem, exigiriam cerca de 400 horas por ano para serem lidas [6, 7], caso os usuários lessem todas as políticas às quais se deparam. No entanto, é justamente por meio desses documentos que o indivíduo compreende — ou deveria compreender — o que será feito com seus dados pessoais pelas plataformas

Além disso, fatores cognitivos e comportamentais levam os usuários a aceitarem termos que não compreendem totalmente, influenciados por vieses e pelo medo de exclusão social [8, 9]. Somado a isso, algumas interfaces exploram fatores cognitivos e utilizam dark patterns. Estes são práticas que manipulam e limitam a autonomia dos indivíduos, levando-os a decisões que não são do seu melhor interesse e podem causar prejuízos [10].

Assim, embora legislações como a LGPD e o GDPR exijam clareza, as plataformas frequentemente falham em tornar as informações acessíveis e equilibradas por meio de suas políticas, comprometendo a efetividade do consentimento [11]. Portanto, o consentimento pode não refletir uma escolha realmente informada, dificultando o exercício dos direitos dos usuários sobre seus dados pessoais.

Diante da complexidade e dos desafios do consentimento e dos fatores que o envolvem em mídias sociais digitais, a representação do conhecimento surge como uma construção conceitual para organizar, estruturar e formalizar as informações relevantes sobre esse domínio. A ontologia, enquanto artefato da representação do conhecimento, permite construir um modelo compreensível por humanos e máquinas, fornecendo uma compreensão clara e compartilhada dos elementos envolvidos no consentimento do titular dos dados [12].

Além de facilitar a interoperabilidade entre sistemas, a ontologia possibilita a atualização contínua frente às rápidas mudanças do ambiente digital, bem como a reutilização e integração com outras bases de conhecimento. Assim, a ontologia não apenas representa o conhecimento, mas o estrutura de modo a apoiar soluções para os desafios do consentimento nas mídias sociais digitais.

Diante do exposto, o presente artigo visa apresentar o desenvolvimento inicial, no âmbito de uma pesquisa de mestrado, de uma estrutura semântica ontológica voltada à representação do consentimento do titular de dados pessoais no contexto das mídias sociais digitais. Além de considerar os aspectos legais brasileiros relacionados à base legal do consentimento, a ontologia proposta também incorpora elementos que influenciam a obtenção desse consentimento. A proposta busca, assim, oferecer um modelo que una aspectos jurídicos e sociocomportamentais.

Este artigo está organizado em seções, conforme a seguir: a seção “Trabalhos Relacionados” apresenta outras ontologias de domínio relacionadas com o escopo do presente estudo; a seção “Metodologia Adotada” descreve detalhadamente as etapas e processos realizados, com vistas à reprodutibilidade científica; a seção “Resultados Parciais” explica a ontologia em desenvolvimento; por fim, a seção “Considerações Parciais e Trabalhos Futuros” finaliza com os últimos comentários sobre o artigo e com as possibilidades de trabalhos futuros.

2. Trabalhos Relacionados

Em uma busca realizada nos repositórios de ontologias BioPortal¹, Ontology Lookup Service², TechnoPortal³, FAIRsharing⁴, OntoHub⁵ e Linked Open Vocabularies⁶, no repositório de código aberto GitHub⁷, e nas bases de dados científicas Web of Science⁸, Scopus⁹ e SciELO¹⁰, foram utilizadas as palavras-chave “*consent ontology*”, “*personal data ontology*”, “*protection ontology*”, “*social media ontology*”, “*GDPR ontology*”, “*LGPD ontology*”. A escolha desses termos visou abranger ontologias relacionadas ao consentimento, à proteção de dados pessoais e ao contexto das mídias sociais digitais, bem como identificar modelos alinhados ao GDPR, que serviu de referência para a legislação brasileira, e à LGPD. Como resultado, foram encontrados os seguintes trabalhos: *GConsent*¹¹, *GDPRov*¹², *Consent Ontology*, *GDPR Ontology*¹³, *Ontology for the Protection of Personal Data (OPPD)*, *PrOnto*, *OntoPriv*, *Ontology for Privacy Policies of OSNs (OPPO)*¹⁴ e o *Data Privacy Vocabulary (DPV)*¹⁵.

A *GConsent* é uma ontologia para representar o consentimento e seus diferentes estados em conformidade com o GDPR [13], sem um contexto de aplicação específica. Essa ontologia não modela aspectos como a finalidade ou a forma de tratamento dos dados. A *GDPRov* [14], a *GDPR Ontology*, a *OPPD* [15] e a *PrOnto* [16] também são ontologias desenvolvidas em conformidade com o GDPR. Enquanto a *GDPRov* representa o fluxo de dados, as demais têm um viés mais jurídico e regulatório. Todas essas quatro ontologias carecem de um contexto de uso definido.

A *Consent Ontology* [17] representa o consentimento com base na Lei de Proteção de Dados Pessoais nº 6.698 da Turquia. A *OntoPriv* [18], por sua vez, tem base na Lei Orgânica de Proteção de Dados Pessoais do Equador, e seu objetivo é assegurar conformidade regulatória. A *OPPO* modela práticas de tratamento de dados descritas nas políticas de privacidade de plataformas de mídias

¹ <https://bioportal.bioontology.org>

² <https://www.ebi.ac.uk/ols4>

³ <https://technoportal.hevs.ch>

⁴ <https://fairsharing.org>

⁵ <https://ontohub.org>

⁶ <https://lov.linkeddata.es/dataset/lov>

⁷ <https://github.com>

⁸ <https://www.webofscience.com/wos>

⁹ <https://www.scopus.com/home.uri>

¹⁰ <https://www.scielo.br>

¹¹ <https://openscience.adaptcentre.ie/ontologies/GConsent/docs/ontology>

¹² <https://openscience.adaptcentre.ie/ontologies/GDPRov/docs/ontology>

¹³ https://github.com/ShahAJh/GDPR_Ontology_Project

¹⁴ <https://github.com/SanondaDattaGupta/OPPO-Ontology>

¹⁵ <https://w3c.github.io/dpv/2.1/dpv>

sociais digitais. Por fim, o DPV é um vocabulário que representa conceitos relacionados à privacidade e proteção de dados, derivados do GDPR.

Não foram encontradas ontologias que modelassem o consentimento de acordo com a LGPD, nem que estabelecessem conexões ou incorporassem aspectos relacionados a fatores que possam influenciar o consentimento fornecido pelo titular, no contexto das mídias sociais digitais.

3. Metodologia Adotada

Esta é uma **pesquisa qualitativa**, de caráter **descritivo** e de natureza **aplicada, com o objetivo geral de sistematizar** o conhecimento sobre o consentimento de indivíduos em mídias sociais digitais, visando apoiar soluções tecnológicas para a privacidade de dados pessoais, a conformidade normativa e a conscientização dos usuários. A metodologia escolhida para o desenvolvimento da ontologia foi a *OntoForInfoScience*, elaborada por Mendonça [19]. Essa metodologia, criada para ser utilizada por profissionais da Ciência da Informação, detalha de maneira simples e em linguagem acessível todas as etapas necessárias para o desenvolvimento de ontologias, superando barreiras encontradas pelos cientistas da informação, como jargões técnicos e questões filosóficas profundas [19].

Além de ser de fácil compreensão, a escolha pela *OntoForInfoScience* também foi motivada pelo seu potencial de contribuir para a disseminação do conhecimento sobre ontologias e do desenvolvimento das mesmas por pessoas que não são especialistas na área, principalmente entre os cientistas da informação. A *OntoForInfoScience* estrutura o processo em oito etapas, além de uma etapa preliminar (etapa 0).

3.1. Etapa 0 - Avaliação da Necessidade da Ontologia

Antes de iniciar o desenvolvimento da ontologia, a *OntoForInfoScience* prevê uma etapa preliminar para avaliar se há realmente uma necessidade para a criação da ontologia, ou se outro instrumento, como um tesouro ou uma taxonomia, seria suficiente para atingir o objetivo proposto [19].

Considerando que o objetivo é a representação do conhecimento de um determinado domínio, avaliou-se que outros instrumentos de recuperação da informação não seriam suficientes para atender à complexidade necessária. Planejou-se uma representação de aspectos do mundo real e a relação entre entidades deste, além de buscar possibilitar o uso em um modelo de mundo aberto, o que vai além das capacidades oferecidas por outros instrumentos.

A motivação também se sustenta na necessidade de explicitar formalmente os conceitos envolvidos, suas propriedades e suas inter-relações. Diferentemente de estruturas mais rígidas, a ontologia permite mais expressividade semântica, favorecendo a representação de significados mais complexos e contextuais. Propõe-se, ainda, que a ontologia seja extensível futuramente e reutilizável em outras ontologias, além de possibilitar inferência automática e aplicação na Web Semântica.

3.2. Etapa 1 - Especificação da Ontologia

A primeira etapa consiste no preenchimento da especificação da ontologia, que é um *template* contendo informações sobre o domínio, o propósito geral, a classe de usuários a que se destina, o uso pretendido, o tipo de ontologia, o grau de formalidade e a delimitação do escopo e as questões de competência [19].

O domínio abrange o **consentimento de indivíduos** em mídias sociais digitais, considerando os aspectos e **os requisitos da LGPD**. Parte-se da definição de consentimento prevista na LGPD, que o estabelece como uma das bases legais para o tratamento de dados pessoais. O propósito é oferecer uma estrutura formal que facilite a compreensão, a análise e a aplicação prática desses conceitos, promovendo a conformidade com a legislação brasileira, além de favorecer o entendimento de aspectos que podem influenciar ou comprometer o consentimento do titular.

Os usuários-alvo incluem pesquisadores das áreas de Ciência da Informação, Direito, Ciência da Computação e Psicologia, profissionais da área de privacidade e proteção de dados, desenvolvedores de sistemas, empresas, órgãos reguladores e o governo. O uso pretendido abrange tanto pesquisas científicas e acadêmicas quanto o desenvolvimento de sistemas e a interoperabilidade de dados com foco na padronização da representação do consentimento. A ontologia é classificada como uma ontologia de domínio, com grau de formalidade médio e estrutura semiformal.

Seu ponto de partida são entidades do mundo real descritas na Basic Formal Ontology (BFO) e o conceito de consentimento conforme definição na LGPD, delimitando-se à hipótese legal de obtenção do consentimento no contexto das mídias sociais digitais, sem abordar aspectos técnicos de implementação nem o tratamento de dados sensíveis ou de crianças e adolescentes. As questões de competência orientam o desenvolvimento da ontologia e incluem perguntas sobre tipos de consentimento, validade, revogação, agentes envolvidos, princípios legais aplicáveis e práticas que comprometem a autonomia do titular.

3.3. Etapa 2 - Aquisição e Extração do Conhecimento

A segunda etapa da metodologia consiste na adoção de métodos para aquisição e extração do conhecimento, com a seleção de fontes de informação [19]. Para essa etapa, foi realizada uma pesquisa bibliográfica e documental com o objetivo de compreender o domínio de estudo.

Por se tratar de uma pesquisa multidisciplinar, a pesquisa bibliográfica também foi conduzida em bases científicas de caráter multidisciplinar: Web of Science, Scopus e SciELO. A busca utilizou as seguintes *strings*: (“*personal data protection*” AND “*consent*”), (“*personal data protection*” AND “*digital social media*”), (“*personal data protection*” AND “*social media*”), (“*consent*” AND “*digital social media*”), (“*consent*” AND “*social media*”), (“*personal data protection*” AND “*consent*” AND “*digital social media*”), (“*personal data protection*” AND “*consent*” AND “*social media*”), (“*proteção de dados pessoais*” OR “*LGPD*”), (“*General Data Protection Regulation*” OR “*GDPR*” OR “*Regulamento Geral sobre a Proteção de Dados*” OR “*RGPD*”). Foram considerados artigos em inglês e português, de acesso aberto. Após a exclusão dos duplicados e o *screening*¹⁶ dos artigos, foram selecionados 55 documentos para serem estudados, com o objetivo de aprofundar a compreensão do domínio.

A pesquisa documental foi realizada por meio da consulta a fontes normativas brasileiras, incluindo a Constituição Federal, a LGPD, o Código Civil, a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor, além de resoluções e outros documentos emitidos pela Autoridade Nacional de Proteção de Dados. Também foram analisados documentos de organizações não governamentais, como o Comitê Gestor da Internet (CGI.br) e a Organização Internacional de Padronização (ISO). Adicionalmente, foram consultadas fontes de organizações internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Visando ao aprofundamento do domínio em estudo e ao entendimento dos aspectos legais das regulamentações que envolvem a área, o processo de extração dos termos candidatos a classes foi realizado de forma manual.

3.4. Etapa 3 - Conceitualização

A próxima etapa refere-se à conceitualização, ou seja, à elaboração da tabela de conceitos e propriedades, do dicionário de verbos e dos modelos conceituais gráficos [19]. Durante essa etapa, foram extraídos 156 termos das fontes de informação, acompanhados de seus respectivos conceitos, compilados em uma planilha eletrônica.

A tabela foi revisada, com a exclusão de termos repetidos e daqueles considerados não pertinentes para uso futuro como classes da ontologia. Ao final, restaram 130 termos. Para cada termo, foram atribuídos, em colunas da planilha eletrônica, os seguintes metadados: ID, **class (EN)**,

¹⁶ Processo de triagem para selecionar e avaliar os estudos que serão incluídos com base nos títulos, resumos e palavras-chave.

label (EN), label (PT), alt label, comment or definition, is defined by, parent, has subclasses, type, object properties e semi-formal definition.

A coluna *object properties* foi construída a partir dos próprios conceitos, como, por exemplo, "[consent is] **deliberately granted by the data subjects**". Essas relações foram organizadas em uma nova planilha, com o objetivo de criar o dicionário de verbos. Para cada relação, foram atribuídos os seguintes metadados: *object property, source ontology, synonyms, inverse property, definition, usage example e characteristics*. Estas últimas referem-se às características das propriedades, tais como simétrica, funcional ou reflexiva.

Os modelos conceituais gráficos, embora façam parte dessa etapa da metodologia, não foram realizados nesse momento, visto que a representação gráfica pode ser criada após a linguagem lógica estar completa e exportada.

3.5. Etapa 4 – Fundamentação Ontológica

A quarta etapa consiste em pesquisar, escolher e aplicar ontologias de fundamentação no desenvolvimento da ontologia. Assim, após uma análise inicial, a BFO foi selecionada como ontologia de fundamentação por oferecer uma estrutura que distingue as entidades entre continuantes (como agentes e dados) e ocorrentes (como os atos de consentimento). **No entanto, embora alguns elementos da BFO tenham sido importados para testes iniciais, a sua integração definitiva e o alinhamento completo ainda não foram concluídos.** Essa incorporação será realizada nas fases subsequentes do desenvolvimento.

3.6. Etapa 5 – Formalização da Ontologia

A quinta etapa consiste na representação formal de todo o conhecimento previamente elaborado, utilizando uma linguagem descritiva ou lógica que permita a interpretação pelas máquinas, favorecendo inferências e a interoperabilidade. Assim, o conhecimento conceitual passa a um nível ontológico-formal [19].

Esta etapa inclui também a pesquisa e a identificação de classes equivalentes em outras ontologias de domínio, visando a integração e a reutilização do modelo desenvolvido. Para isso, foram consultados repositórios e portais de ontologias, como BioPortal, Linked Open Vocabularies, Ontology Lookup Service, OntoHub e GitHub. A partir dessa análise, as classes consideradas compatíveis com o escopo da ontologia foram adicionadas na coluna "termos similares" da tabela de conceitos e propriedades.

Para a etapa de formalização, foi utilizado o software Protégé, versão 5.6.5. O processo teve início com a inserção dos termos, dados e metadados da tabela de conceitos e propriedades, bem como as relações identificadas no dicionário de verbos. Também foram importadas as classes equivalentes de outras ontologias de domínio, previamente identificadas.

A última parte consistiu na adição de axiomas, quando pertinentes, com a especificação de restrições e relações entre as classes e propriedades. Por exemplo, definiu-se que a classe **ConsentGiven**, subclasse de **gc:ConsentStatusValidForProcessing**, é equivalente à interseção simultânea das classes **FreeConsent**, **UnequivocalConsent** e **InformedConsent**. Além disso, o **ConsentGiven** deve ser concedido (por meio da propriedade **isGrantedBy**) por exatamente um indivíduo pertencente à classe **DataSubject**. Em outras palavras, o tratamento de dados é permitido quando o consentimento dado pelo titular é livre, informado e inequívoco.

3.7. Etapa 6 – Avaliação da Ontologia

A sexta etapa corresponde à avaliação da ontologia, composta pelas fases de validação - que avalia a adequação da ontologia em relação ao domínio representado - e de verificação, que avalia a consistência ontológica, ambas realizadas com base em critérios avaliativos [19].

Conforme recomendado na própria metodologia *OntoForInfoScience*, foram utilizados os *reasoners* HermiT e Pellet, disponíveis no próprio Protégé, para a validação lógica e para a verificação de problemas de imprecisão e inconsistência nas relações semânticas. As inconsistências

apontadas pelos *reasoners* foram analisadas, revisadas e corrigidas. Além disso, a ontologia passou por uma revisão com consulta a outros pesquisadores, com o objetivo de assegurar a qualidade conceitual e a aderência aos requisitos do domínio.

3.8. Etapas 7 e 8 - Documentação e Disponibilização da Ontologia

As duas últimas etapas devem ser realizadas após a conclusão efetiva de todas as etapas anteriores, consistindo na documentação formal, em linguagem natural, de todas as informações contidas na ontologia e, por fim, na disponibilização da ontologia em linguagem lógica, apresentada em meio eletrônico [19].

O desenvolvimento da proposta apresentada neste artigo ocorreu entre janeiro e julho de 2025. Até a data limite para a submissão deste artigo, a pesquisa encontrava-se em fase final de desenvolvimento. Portanto, a documentação final ainda está em fase de elaboração e a ontologia ainda não foi disponibilizada publicamente. Contudo, planeja-se disponibilizá-la em acesso aberto, em formato *Web Ontology Language* (OWL), por meio de um repositório de dados.

4. Resultados Parciais

A pesquisa bibliográfica e documental resultou na extração e na formalização de 130 classes para compor a base conceitual da ontologia. A organização hierárquica dessas classes (figura 1) estrutura-se em eixos principais para a representação do conhecimento, tais como: o agente e seus processos cognitivos (ex: *foaf:Agent*, *CognitiveBias*, *RationalDecision*), as plataformas de mídias sociais e seus mecanismos (ex: *OnlinePlatform*, *ControlMechanism*, *DarkPattern*), os instrumentos normativos e informativos (ex: *Legislation*, *LegalBasis*, *PolicyDocument*, *Notice*); e o tratamento de dados (ex: *Data*, *Processing*, *dpr:ConsentStatus*). Essa estruturação visa representar de forma conectada os diversos elementos que permeiam o consentimento do titular.

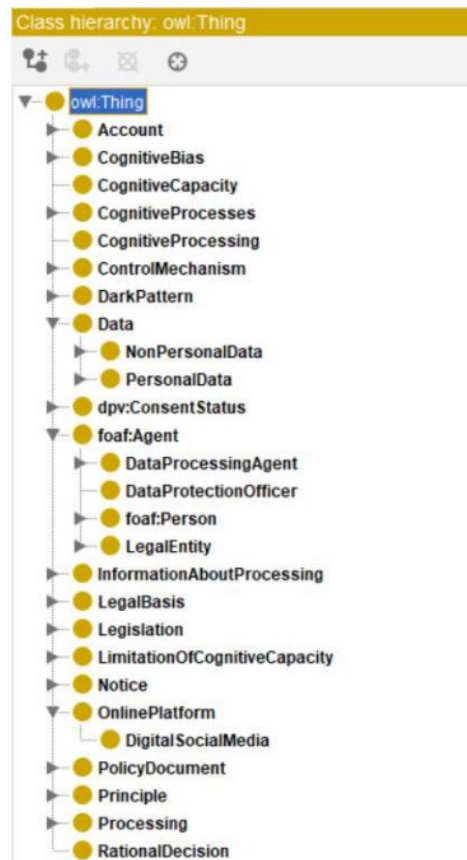


Figura 1: Disposição hierárquica de parte das classes da ontologia mostrada na aba class hierarchy no Protégé.

4.1. O Consentimento

O conceito central da ontologia é a classe **Consent** (figura 2) que representa a concordância do titular para o tratamento de seus dados pessoais [5], e figura como uma subclasse de **LegalBasisUnderLGPD**. Para que o consentimento seja considerado válido, ele precisa ser livre, informado e inequívoco [5]. A intersecção dessas qualificadoras (**FreeConsent**, **InformedConsent** e **UnequivocalConsent**) resulta na classe **ConsentGiven**, que é concedido por exatamente um **DataSubject**.

Utilizando classes importadas do DPV e da GConsent, também são modelados os diferentes status que o consentimento pode assumir. A classe *dpv:ConsentStatus* é especializada em *gc:ConsentStatusValidForProcessing* e *gc:ConsentStatusInvalidForProcessing*. Enquanto o tratamento de dados (*Processing*) só pode ser realizado sob uma única condição, um *ConsentGiven*, o tratamento não pode ser efetuado nas seguintes condições [5]: *ConsentRefused*, quando o titular não aceita o tratamento; *ConsentWithdrawn*, quando o titular retira o consentimento previamente dado; *NullConsent*, quando as informações fornecidas ao titular sobre o tratamento são enganosas ou não transparentes; e *ConsentVitiated*, quando o consentimento é obtido por meio de defeitos do negócio jurídico (coerção, dolo, erro, estado de perigo).

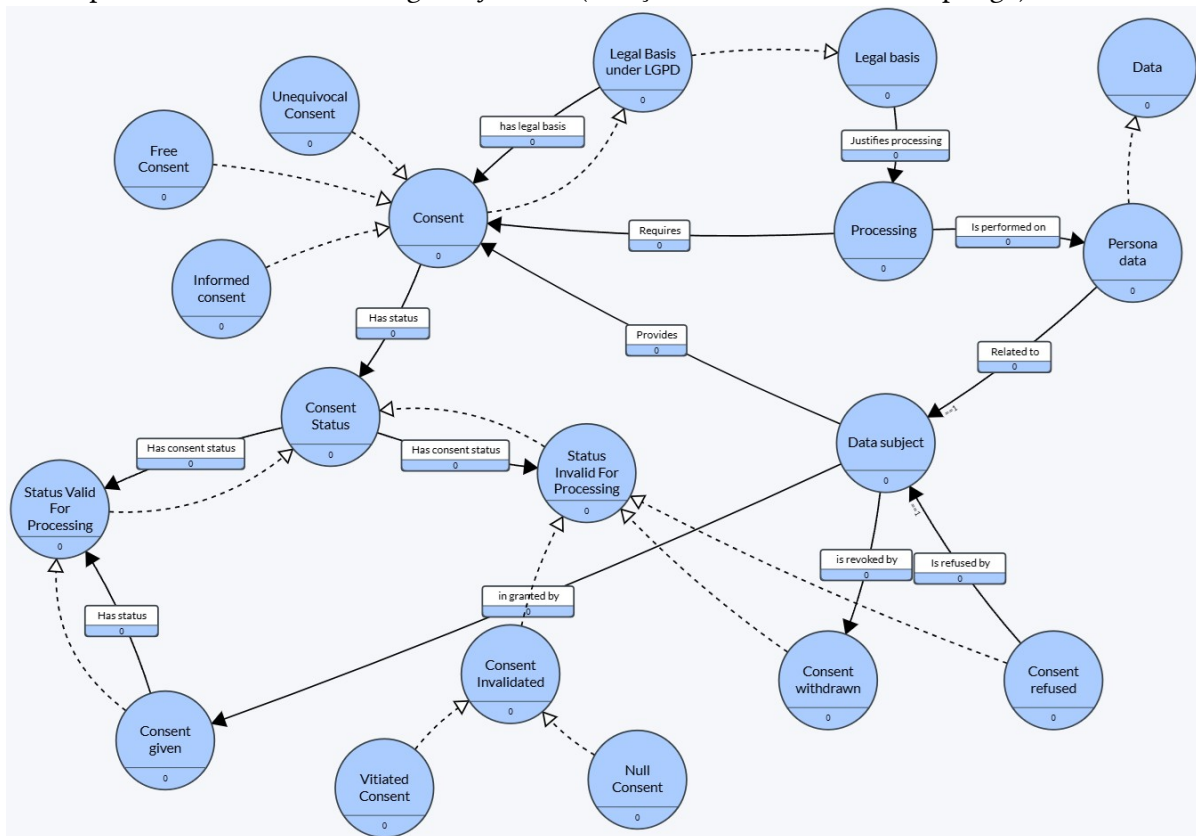


Figura 2: Diagrama que modela o consentimento como base legal para o tratamento de dados pessoais, destacando seus tipos, estados e relações com o titular dos dados segundo a LGPD.

4.2. O Titular de Dados e seus Aspectos Cognitivos

O consentimento é articulado em torno de uma figura central: o **DataSubject**, que é a pessoa a quem se referem os dados pessoais que são objeto de tratamento [5]. Nesse contexto, o **DataSubject** é uma subclasse de **NaturalPerson**, que, por sua vez, é subclasse de **foaf:Person** e **foaf:Agent**. No contexto específico das mídias sociais digitais, o usuário de mídias sociais digitais (**DigitalSocialMediaUser**) é uma especificação de **DataSubject**.

A ontologia dedica atenção aos aspectos cognitivos que podem influenciar a capacidade do titular de dados de fornecer um consentimento verdadeiramente livre, informado e inequívoco (figura 3). A classe **CognitiveCapacity** representa a capacidade cognitiva e, também, os limites ao

processamento cognitivo, que são processos mentais que a mente utiliza para processar e organizar informações [20]. As limitações dessa capacidade são modeladas pela classe **LimitationOfCognitiveCapacity**, que pode tornar o processo de tomada de decisão (**DecisionMakingProcess**) mais difícil e influenciar uma decisão racional (**RationalDecision**).

Adicionalmente, a ontologia modela a classe **CognitiveBias**, que são distorções cognitivas que podem desviar a percepção, o julgamento e a tomada de decisão [21]. As subclasses de vieses cognitivos necessitam de expansão. No momento, englobam somente as classes **DefaultBias**, **FreeBias** e **PresentBias**.

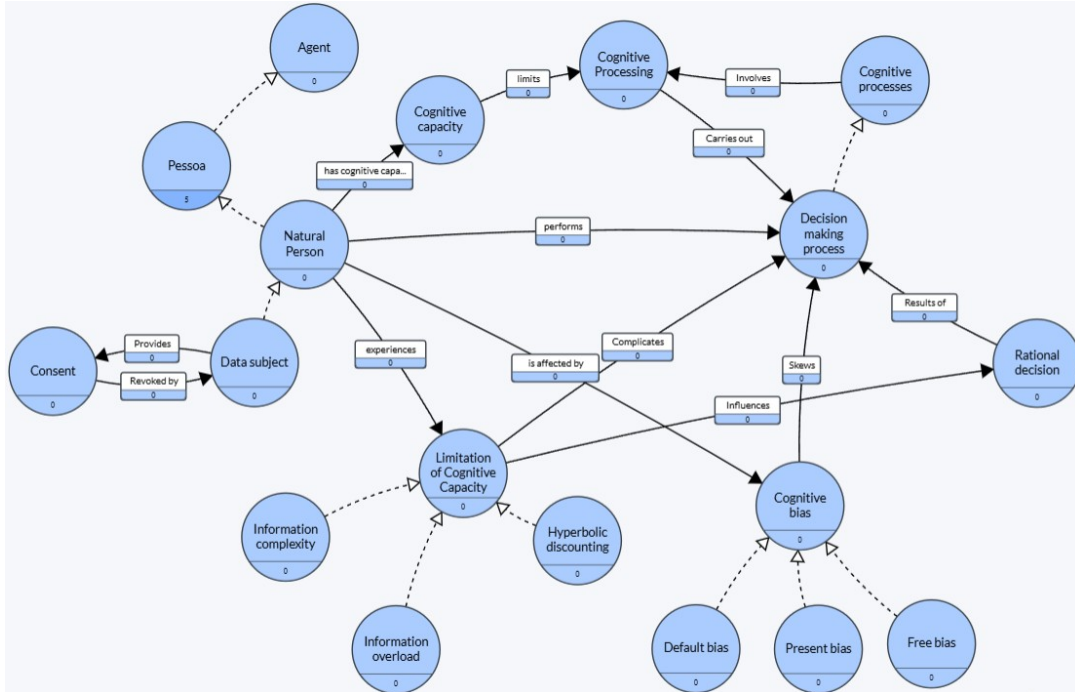


Figura 3: Diagrama que modela as limitações cognitivas e vieses que afetam o processo decisório da pessoa natural na concessão do consentimento.

4.3. Mídias Sociais Digitais e seus Mecanismos

No escopo deste trabalho, a interação do titular para fins de consentimento ocorre em mídias sociais digitais (**DigitalSocialMedia**), que são uma subclasse de **OnlinePlatform**. O **DigitalSocialMediaUser** está ligado a essas plataformas por meio da posse de uma conta (**DigitalSocialMediaAccount**) nelas.

A ontologia também representa os mecanismos presentes nas plataformas que gerenciam as preferências de consentimento (figura 4). A classe **ConsentMechanism** tem a subclasse **ConsentManagement**, que são sistemas ou processos que permitem aos usuários determinarem quais informações eles permitem que sejam acessadas [22]. Um exemplo é o mecanismo **OptIn**, que exige uma ação afirmativa do usuário para a concessão do consentimento [23].

Um foco particular da ontologia é a representação da classe **DarkPattern**, definido como interfaces implementadas nas plataformas que tentam influenciar os usuários a tomarem decisões não intencionais, involuntárias e potencialmente prejudiciais em favor dos interesses das plataformas [24]. São detalhados os seguintes tipos de *dark patterns*: **Fickle**, caracterizado por uma interface inconsistente e não clara; **LeftInTheDark**, quando a interface é projetada para ocultar informações; **Obstructing**, quando as interfaces dificultam o gerenciamento de dados; **Overloading**, quando o usuário se depara com uma sobrecarga de informações; **Skipping**, caracterizado pelo *design* projetado de forma que os usuários esqueçam sobre a proteção de dados; e **Stirring**, que afeta a escolha do usuário ao apelar para as suas emoções [24].

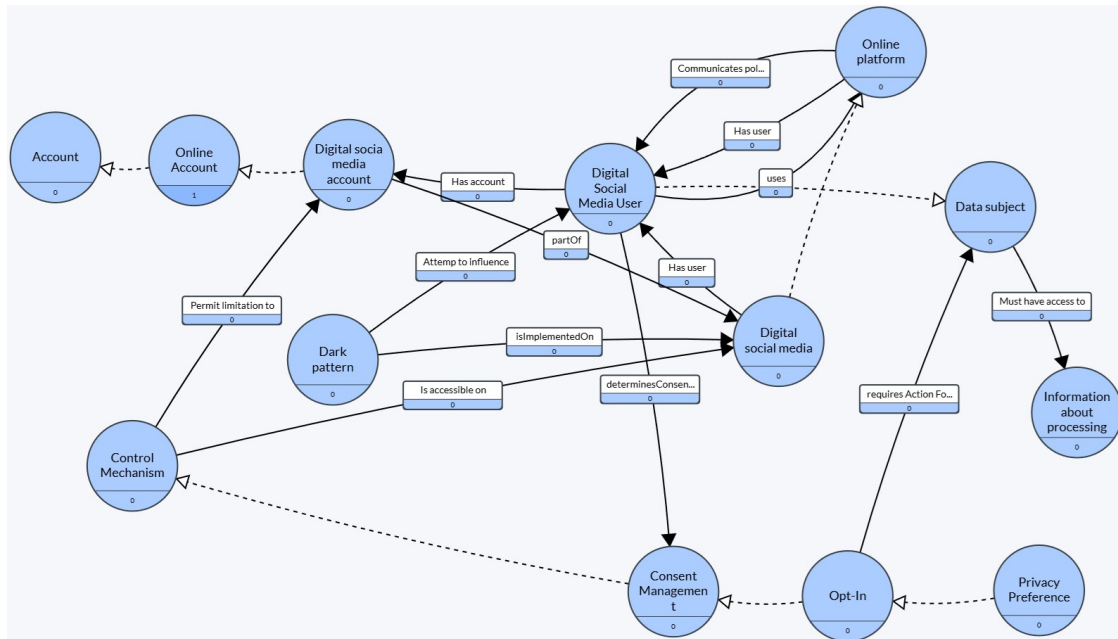


Figura 4: Diagrama representando as relações entre usuários, plataformas e mecanismos de consentimento em mídias sociais digitais.

4.4. Arcabouço Legal-Normativo e Informativo

A classe **Legislation** especializa-se em **BrazilianLegislation**, que, por sua vez, tem como instância a LGPD e o Código Civil Brasileiro. O Código Civil define os vícios do negócio jurídico, como erro, dolo ou coação, que podem invalidar o consentimento, caracterizando o vício de consentimento, um tipo de consentimento inválido para o tratamento de dados [5]. Além disso, o Código também trata da capacidade jurídica necessária para que o negócio jurídico seja válido, exigindo a livre manifestação da vontade. A LGPD, por sua vez, é referência para estabelecer as hipóteses legais para o tratamento de dados pessoais, representadas pela classe **LegalBasisUnderLGPD**, que é uma especialização de **LegalBasis**. Dentro do domínio da ontologia, a classe **Consent** é modelada como uma das hipóteses legais prevista na LGPD (figura 5).

Os princípios que o tratamento de dados pessoais deve observar são representados como subclasses de **PrincipleUnderLGPD**, que por sua vez é uma especialização de **Principle**. A ontologia representa os seguintes princípios: **Purpose**, **Adequacy**, **Necessity**, **FreeAccess**, **DataQuality**, **Transparency**, **Security**, **Prevention**, **NonDiscrimination**, **Accountability** e **Liability** [5]. Além disso, também são representados os diferentes tipos de operações de tratamento de dados.

Também são representados os agentes no ciclo de tratamento de dados pessoais, subclasses da classe **foaf:Agent**. Os agentes de tratamento são o **Controller**, que é o responsável pelas decisões sobre o tratamento, e o **Processor**, que efetua o tratamento em nome do controlador [5]. O **DataProtectionOfficer** atua como canal de comunicação entre o **Controller**, o **DataSubject** e a **NationalAuthority** [5], representada pela Autoridade Nacional de Proteção de Dados.

A ontologia também estrutura as informações que devem ser fornecidas ao titular dos dados para a obtenção de um consentimento válido. As informações incluem a duração e a forma de tratamento, as informações do controlador, as responsabilidades do agente e os direitos do titular. Os direitos dos titulares são agrupados sob a classe **DataSubjectRight**.

Por fim, é representada a classe **PolicyDocument**, que corresponde aos documentos disponibilizados pelas mídias sociais digitais. Essa classe é subdividida em **PrivacyPolicy** e **TermsAndConditions**. A ontologia estabelece que uma mídia social digital deve possuir tais documentos, e que estes devem ser acessíveis aos usuários. A **PrivacyPolicy** descreve as operações de tratamento de dados e deve fornecer todas as informações sobre o tratamento ao **DataSubject**, aspecto essencial para a validade do consentimento.

Agradecimentos

Agradecemos ao Programa de Pós-Graduação em Gestão da Informação (PPGGI) da Universidade Federal do Paraná (UFPR) pelo suporte à realização deste trabalho. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES), por meio de recursos do PROAP, Edital nº 28/2025 – SA/PPGGI.

Declaração de IA Generativa

Durante a preparação deste trabalho, os autores utilizaram o GPT-4 para: Verificação gramatical e ortográfica. Após a utilização da ferramenta, os autores revisaram e editaram o conteúdo conforme necessário e assumem responsabilidade total pelo conteúdo da publicação.

Referências

- [1] D. S. Paulichi, V. S. G. Cardin, Dinâmicas da sociedade informacional contemporânea: análise da captação de dados em plataformas digitais e suas implicações socioculturais, *Pensar* 29 (2024) 1–14. doi:10.5020/2317-2150.2024.14816.
- [2] N. F. D. M. Maciel, A globalização das plataformas digitais: uma análise sobre a necessidade de regulamentação dessa ferramenta, *Rev. Foco* 16 (2023) e3092. doi:10.54751/revistafoco.v16n10-155.
- [3] X. Ye, Y. Yan, J. Li, B. Jiang, Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective, *Telecommunications Policy* 48 (2024) 102851. doi:10.1016/j.telpol.2024.102851.
- [4] European Parliament and Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, vol. L119, pp. 1–88, May 2016. URL: <https://gdpr-info.eu>.
- [5] Brazil. Law No. 13,709, August 14, 2018 — General Data Protection Law (LGPD). *Official Gazette of the Union*, Brasília, 2018. URL: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
- [6] V. Belcheva, T. Ermakova, B. Fabian, Understanding Website Privacy Policies—A Longitudinal Analysis Using Natural Language Processing, *Information* 14 (2023) 622. doi:10.3390/info14110622.
- [7] X. Ding, H. Huang, For whom is privacy policy written? A new understanding of privacy policies, *Computer Law & Security Review* 55 (2024) 106072. doi:10.1016/j.clsr.2024.106072.
- [8] L. Wolmarans, A. Voorhoeve, What Makes Personal Data Processing by Social Networking Services Permissible?, *Canadian Journal of Philosophy* 52 (2022) 93–108. doi:10.1017/can.2022.4.
- [9] L. N. Lugati, J. E. D. Almeida, Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa, *RD* 12 (2020) 01–33. doi:10.32361/2020120210597.
- [10] OECD. Dark commercial patterns. *OECD Digital Economy Papers*, no. 336, OECD Publishing, Paris, 2022. URL: <https://doi.org/10.1787/44f5e846-en>.
- [11] D. Green, Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation, *International Journal for the Semiotics of Law* 38 (2025) 701–729. doi:10.1007/s11196-024-10132-4.
- [12] M. B. Almeida, *Ontologia em Ciência da Informação: Teoria e Método*, vol. 1, Coleção Representação do Conhecimento em Ciência da Informação, Editora CRV, Curitiba, Brazil, 2020. ISBN 978-65-5578-679-8. doi:10.24824/978655578679.8.
- [13] H. J. Pandit, C. Debruyne, D. O’Sullivan, D. Lewis, GConsent – A Consent Ontology Based on the GDPR, in: P. Hitzler, M. Fernández, K. Janowicz (Eds.), *The Semantic Web: Proceedings of the 16th International Conference, ESWC 2019, Portorož, Slovenia, June 2–6, 2019*, volume

- 11503 of Lecture Notes in Computer Science, Springer, Cham, 2019, pp. 270–282. doi:10.1007/978-3-030-21348-0_18.
- [14] H. J. Pandit, D. Lewis, Modelling Provenance for GDPR Compliance using Linked Open Data Vocabularies, in: F. Scharffe, F. Schneider (Eds.), Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web – Policy and Technology (PrivOn 2017), co-located with ISWC 2017, volume 1951 of CEUR Workshop Proceedings, CEUR-WS.org, Vienna, Austria, 2017. URL: https://ceur-ws.org/Vol-1951/PrivOn2017_paper_6.pdf.
 - [15] M. El Ghosh, H. Abdulrab, Capturing the Basics of the GDPR in a Well-Founded Legal Domain Modular Ontology, *Frontiers in Artificial Intelligence and Applications* 344 (2021) 144–158. doi:10.3233/FAIA210378.
 - [16] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, L. Robaldo, PrOnto: Privacy Ontology for Legal Reasoning, in: A. Kő, E. Francesconi (Eds.), *Electronic Government and the Information Systems Perspective. EGOVIS 2018*, Springer, Cham, 2018, pp. 101–115. doi:10.1007/978-3-319-98349-3_11.
 - [17] E. Olca, O. Can, DICON: A Domain-Independent Consent Management for Personal Data Protection, *IEEE Access* 10 (2022) 95479–95497. doi:10.1109/ACCESS.2022.3204970.
 - [18] G. Suntaxi, K. Ojeda, F. Rodríguez, OntoPriv: Enhancing Understanding and Compliance in Privacy Legislation via Legal Ontologies, in: *Proceedings of the 2024 Latin American Computer Conference (CLEI)*, IEEE, Buenos Aires, Argentina, 2024, pp. 1–10. doi:10.1109/CLEI64178.2024.10700326.
 - [19] F. M. Mendonça, OntoForInfoScience: metodologia para construção de ontologias pelos cientistas da informação - uma aplicação prática no desenvolvimento da ontologia sobre componentes do sangue humano (Hemonto), Ph.D. thesis, Federal University of Minas Gerais, Belo Horizonte, MG, Brazil, 2015. URI: <http://hdl.handle.net/1843/BUBD-A35H3K>.
 - [20] D. Krch, Cognitive processing, in J. S. Kreutzer, J. DeLuca, and B. Caplan (Eds.), *Encyclopedia of Clinical Neuropsychology*, New York, NY: Springer, 2011, p. 627, doi: 10.1007/978-0-387-79948-3_1443. URL: https://link.springer.com/referenceworkentry/10.1007/978-0-387-79948-3_1443.
 - [21] APAONTO – Ontologia sobre aspectos psicológicos e jurídicos do consentimento. NCBO BioPortal, 2024. URL: <https://bioportal.bioontology.org/ontologies/APAONTO>.
 - [22] N. Almeida, M. Silva, A Blockchain-Based Hybrid Architecture for Auditable Consent Management, *IEEE Transactions on Industrial Informatics* 19 (2023) 2654–2662. doi:10.1109/TII.2023.10604861.
 - [23] Associação Brasileira de Normas Técnicas – ABNT. NBR ISO/IEC 29100:2024 – Tecnologia da informação – Técnicas de segurança – Arquitetura de privacidade, Rio de Janeiro: ABNT, 2024.
 - [24] European Data Protection Board – EDPB. Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, versão final, Bruxelas, 24 fev. 2023. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.